REMARKS:

Claims 1, 9, 11, 13, 16, 17 and 22-26 are in the case and presented for consideration.

This amendment after final is being filed with an RCE and the required fee. The Commissioner is further authorized to charge Deposit Account No. 14-1431 for any additional fees which may now be due under 37 C.F.R. 1.16 or 1.17.

The Applicants thank the Examiner for the acceptance fo the corrections to the specification.

Claims 1, 13, 16, 17 and 22-26 have been rejected as being fully anticipated by US Patent 6,721,886 to Uskela and claims 9 and 11 have been rejected as being obvious form Uskela in view of US Patent 6,487,667 to Brown.

For the reasons set forth below, it is believed that the claims as now amended are patentable over these references and that the application and claims are in condition for allowance.

According to the claimed invention, the response to the challenge is generated using access privilege proving data that is created from the private key corresponding to the public key assigned to the service of the server.

In this configuration, access privilege proving data is in advance prepared from the private key that si unique to the service of the server. The client is allowed to access to the service only when the client has the corresponding privilege proving data for that service. The client can show access privilege to each service using individual privilege proving data. The client does not need to have corresponding unique operations to different services.

In this regard, the claim 1 recites, among other things:

"an access privilege verifier for verifying, using a corresponding public key, whether a prescribed relationship exists between the challenge and a response to that challenge received from the client;

wherein the response is calculated based on a unique operation for the client and access privilege proving data that is created from a private key corresponding to the public key assigned to the each service of the server."

Also, claim 25 recites, among other things:

"an access privilege proving data storage unit that stores access privilege proving data, the access privilege proving data being created from a private key corresponding to a public key assigned to the requested service and result of a same unique operation to one executed by the unique operation executor;

a response generator that generates the response to the challenge, the challenge being received from the server, and

wherein the response is calculated based on result of the unique operation and the access privilege proving data, and unique operation is unique to the client."

The remaining claims have same limitations.

In contrast, Uskela only discloses a secure system in which a service provider sends a random number as a challenge to a user, the user encipher the random number by the user's private key to produce the response, and then the provider decipher the response by the user's public key and compare the deciphered response against the challenge.

With Uskela, in order to provide each access control for each service, user must have different private keys corresponding to the different services and also the server must have corresponding public keys to the different private keys owned by the user. The user must keep those private keys securely. In the claimed invention here, the client must have only one unique operation which must be securely stored. In order to enable individual access control for many services, the client must only have corresponding privilege proving data units which need not be stored securely.

Brown also does not disclose or suggest these features of the claimed invention so that a combination of Uskela and Brown would not render the claims obvious.

Further, it is respectfully submitted that in Uskele, users use a common encryption operation, and only use different private keys. It is easy to copy a private key and give it to another, and when the user's private key is copied for illegal use, there are no means to prevent such unauthorized use.

In summary, no prior art discloses the generation of response to challenge based on a unique operation for the client and access privilege proving data that is created from a private key corresponding to the public key assigned to the each service of the server, which enables different access controls for different services using only one unique operation to the client, and prohibits unauthorized access using an unauthorized copy of data, for example, a user's private key.

Therefore, the applicants' invention is believed to be patentably distinguishable over the prior art.

If any issues remain, the Examiner is respectfully invited to contact the undersigned at the number below.

Further favorable action is respectfully requested.

Peter C. Michalos
Reg. No. 28,643
Attorney for Applicants
(845) 359-7700

Dated: January 10, 2006

NOTARO & MICHALOS P.C.
100 Dutch Hill Road, Suite 110
Orangeburg, New York 10962-2100

Customer No. 21706